UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/734,330	11/30/2000	Alex O. Agerholm	10559/382001/P10188	3827

20985 7590 02/23/2004

FISH & RICHARDSON, PC
12390 EL CAMINO REAL
SAN DIEGO, CA 92130-2081

EXAMINER	
KENNEDY, LESA M	

ART UNIT	PAPER NUMBER
2151	6

DATE MAILED: 02/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/734,330	Applicant(s) AGERHOLM ET AL.	
	Examiner Lesa Kennedy	Art Unit 2151	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 November 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 March 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Remarks

1. This action is responsive to the application filed on November 30, 2000. Claims 1-24 are pending examination. Claims 1-24 are directed towards a system and method for communicating SNMP information using an HTTP protocol.

2. The abstract contains grammatical/typographical errors on lines 7 and 9. Appropriate correction is recommended.

3. The specification contains a grammatical/typographical error on page 4, line 22. Appropriate correction is recommended.

4. Reference item 315 in Fig. 3A contains a grammatical/typographical error. Appropriate correction is recommended.

Drawings

5. The drawings are objected to because:

- Items 105 and 110 in Fig. 1 do not have descriptive labels.
- Fig. 1 contains a block that it not labeled or numbered.
- The specification makes reference to item 135 in Fig. 1 (see pg. 3, line 5), however this item is not identified in the figure.

A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Specification

6. The disclosure is objected to because of the following informality:

The Detailed Description section makes reference to item 15 in Figure 2 (see page 4, line 2), however there is no reference item labeled 15 in Figure 2.

Appropriate correction is required.

Claim Objections

7. Claims 7 and 19 are objected to because of the following informalities:

- Claim 7 refers to 'said first monitored computer' (line 9). This reference lacks antecedent basis. For purposes of further reviewing this claim, it will be assumed that the applicant is referring to the 'first monitoring computer' (line 4).
- Claim 19 refers to 'said SNMP information' (line 23). This reference lacks antecedent basis. For purposes of further reviewing this claim, it will be assumed that the applicant is referring to the 'encapsulated SNMP information' (line 22), and not to the 'SNMP format network information' on line 20.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schlener et al. (U.S. Patent No. 6,182,157) in view of Kannan et al. (U.S. Pub No. 2001/0054064).

Schlener teaches the invention substantially as claimed including a method and apparatus for monitoring the status of a network device (see abstract).

As to claim 1, Schlener teaches a method comprising:

obtaining, at a first node, information indicative of a network condition (col. 3, line 66 – col. 4, line 6; Schlener discloses that agents on managed network elements detect events); and

sending said information to a network managing node (col. 4, line 3; Schlener discloses that a manager receives event notifications from the agents).

However, Schlener fails to teach the limitation of encapsulating said information into an HTTP protocol.

However, Kannan teaches a method for secure communication between a customer and a CSR via a web server (see abstract). Kannan teaches the limitation of encapsulating information into an HTTP protocol (par. 0126; Kannan discloses encapsulating data into HTTP messages).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Schlener in view of Kannan by applying HTTP encapsulation to the event information. One would be motivated to do so to provide secure transmission of the data.

As to claim 2, the combination of Schlener in view of Kannan teaches the method of claim 1, wherein said information is SNMP information (col. 4, line 15; Schlener discloses that the agents are SNMP agents).

As to claim 3, the combination of Schlener in view of Kannan teaches the method of claim 1, wherein said HTTP protocol is an HTTPs protocol (par. 0129; Kannan discloses that any HTTP compatible security technique (e.g. secure HTTP) may be used).

As to claim 4, the combination of Schlener in view of Kannan teaches the method of claim 1, wherein said encapsulating comprises forming an HTTP message including said information (par. 0126; Kannan discloses that encapsulated data is passed in HTTP messages).

As to claim 5, the combination of Schlener in view of Kannan teaches the method of claim 1, wherein said information is textual information, and wherein said encapsulating comprises forming an HTTP message including said textual information therein (col. 1, lines 41-45; Schlener discloses that in SNMP, text strings are used to represent managed data variables) (par. 0126; Kannan discloses that encapsulated data is passed in HTTP messages).

As to claim 6, the combination of Schlener in view of Kannan teaches the method of claim 5, wherein said HTTP message includes tags (par. 0126; Kannan discloses that the HTTP message is tagged).

As to claim 7, the combination of Schlener in view of Kannan teaches a system, comprising:

a first, monitoring computer, running a first program that monitors a network connection (col. 3, line 63 – col. 4, line 9; Schlener discloses a management software running on a management station which monitors network elements);

a second, monitored computer, running a second program which allows said first program to monitor some aspect of the network connection (col. 3, line 63 – col. 4, line 9; Schlener discloses that network elements include an agent software which gathers monitoring data for the management station);

a connection between said first and second monitored computers (col. 3, line 60; Schlener discloses network connections between the management station and the network elements), said connection including a firewall which blocks at least some kinds of communications but does not block HTTP communications (par. 0126; Kannan discloses the use of firewalls that allow HTTP traffic to pass); and

at least one of said first and second computers running a third program that encapsulates information into HTTP protocol (par. 0126; Kannan discloses the use of HTTP communicators to encapsulate data into HTTP protocol).

As to claim 8, the combination of Schlener in view of Kannan teaches the system of claim 7 wherein said third program is part of one of said first and second programs (par. 0072, 0074; Kannan discloses a web server comprising an agent which comprises an HTTP communicator).

As to claim 9, the combination of Schlener in view of Kannan teaches the system of claim 7 wherein said first and second programs each operate based on SNMP protocol (col. 4, line 2; Schlener discloses that the manager and agents communicate using SNMP protocol).

As to claim 10, the combination of Schlener in view of Kannan teaches the system of claim 7 wherein said HTTP information is HTTPs information (par. 0129; Kannan discloses that any HTTP compatible security technique (e.g. secure HTTP) may be used).

As to claim 11, the combination of Schlener in view of Kannan teaches the system of claim 9, wherein said encapsulating comprises forming tags in the HTTP (par. 0126; Kannan discloses that the HTTP message is tagged).

As to claim 12, the combination of Schlener in view of Kannan teaches a method comprising:

forming an SNMP request for information from a remote computer, in a management station computer (col. 4, line 2; Schlener discloses that a manager sends SNMP requests to network elements);

changing a request to a form which will be passed by a firewall as a changed request (par. 0126; Kannan discloses that data is HTTP encapsulated to allow it to pass through firewalls); and

sending said changed request to said remote computer through said firewall (col. 4, line 2; Schlener discloses that a manager sends SNMP requests to network elements; par. 0126; Kannan discloses that data is HTTP encapsulated to allow it to pass through firewalls).

As to claim 13, the combination of Schlener in view of Kannan teaches the method of claim 12, wherein said changed SNMP request is an SNMP request which is encapsulated into HTTP protocol (col. 4, line 2; Schlener discloses that a manager sends SNMP requests to network elements; par. 0126; Kannan discloses that data is HTTP encapsulated to allow it to pass through firewalls).

As to claim 14, the combination of Schlener in view of Kannan teaches the method of claim 13 wherein said HTTP protocol includes a secure socket layer (par. 0129; Kannan discloses that communication security is provided through a secure socket layer).

As to claim 15, the combination of Schlener in view of Kannan teaches the method of claim 13, wherein said changed request includes tags in a style usually used by said HTTP protocol (par. 0126; Kannan discloses that the HTTP message is tagged).

As to claim 16, the combination of Schlener in view of Kannan teaches the method of claim 12 further comprising:

receiving said changed SNMP request in said remote computer (col. 4, line 2; Schlener discloses that a manager sends SNMP requests to network elements; par. 0126; Kannan discloses that data is HTTP encapsulated to allow it to pass through firewalls); and

changing said changed SNMP request into a standard SNMP request (par. 0126; Kannan discloses that received messages are deencapsulated).

As to claim 17, the combination of Schlener in view of Kannan teaches the method of claim 16 further comprising:

in said remote computer, preparing an SNMP response (col. 3, line 66 – col. 4, line 9; Schlener discloses that network elements send operational data and detected event information to the management station);

encapsulating a response as a changed response (par. 0126; Kannan discloses that data is HTTP encapsulated to allow it to pass through firewalls); and

sending said changed SNMP response through said firewall to said management station computer (col. 3, line 66 – col. 4, line 9; Schlener discloses that network elements send

operational data and detected event information to the management station; par. 0126; Kannan discloses that data is HTTP encapsulated to allow it to pass through firewalls).

As to claim 18, the combination of Schlener in view of Kannan teaches the method of claim 17 further comprising changing a changed response to a standard response (par. 0126; Kannan discloses that received messages are deencapsulated).

As to claim 19, the combination of Schlener in view of Kannan teaches a computer program, embodied on tangible program media, containing instructions causing a computer to:

detect SNMP format network information (col. 3, line 66 – col. 4, line 9; Schlener discloses that network elements send operational data and detected event information to the management station);

encapsulate information into an HTTP format as encapsulated information (par. 0126; Kannan discloses that data is HTTP encapsulated to allow it to pass through firewalls); and

send said SNMP information to a remote location (col. 3, line 66 – col. 4, line 9; Schlener discloses that network elements send operational data and detected event information to the management station; par. 0126; Kannan discloses that data is HTTP encapsulated to allow it to pass through firewalls).

As to claim 20, the combination of Schlener in view of Kannan teaches the program of claim 19, wherein said SNMP format network information is an SNMP request (col. 4, line 3; Schlener discloses that a manager requests operational data from agents).

As to claim 21, the combination of Schlener in view of Kannan teaches the program of claim 19 wherein said SNMP format information is an SNMP response (col. 4, lines 3-9;

Schlener discloses that agents send operational data to the management station for interpretation).

As to claim 22, the combination of Schlener in view of Kannan teaches the program of claim 19 wherein said HTTP format is an HTTPs format (par. 0129; Kannan discloses that any HTTP compatible security technique (e.g. secure HTTP) may be used).

As to claim 23, the combination of Schlener in view of Kannan teaches the program of claim 19 wherein said instructions further cause the computer to encapsulate said information using a secure socket layer (par. 0129; Kannan discloses that communication security is provided through a secure socket layer).

As to claim 24, the combination of Schlener in view of Kannan teaches the program of claim 19 wherein said encapsulating comprises forming HTML tags representing SNMP information (par. 0126; Kannan discloses that the HTTP message is tagged).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Lesa Kennedy whose telephone number is (703) 305-8865. The examiner can normally be reached on Monday - Friday, 8:30 am - 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glenton Burgess can be reached on (703) 305-4792. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Andrew Caldwell
Andrew Caldwell

Lesa Kennedy
Art Unit 2151